UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/528,562	10/28/2005	Takehiko Nakano	266812US6PCT	6309

22850   7590   12/17/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
SHOLEMAN, ABU S

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
12/17/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

	Application No.	Applicant(s)
Office Action Summary	10/528,562	NAKANO ET AL.
	Examiner	Art Unit	
	ABU SHOLEMAN	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09/30/2009*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-14,16-19,21-23,25- 26* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-14,16-19,21-23,25 and 26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
         application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *10/29/2009*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

11/10/2009 has been entered.

2.   Claims 1, 3-4, 16, 18, 19, 21-23, and 26 are amended by the present

amendment.

Response to Amendment

3.   Applicant's arguments, see pages 1-6, filed on 09/30/2009, with respect to the

rejection(s) of claim(s) 1, 3-4, 16, 18, 19, 21-23, and 26 under 35 U.S.C § 103(a), have

been fully considered but are moot in view of the new ground(s) of rejection .

Claim Objections

4.   Claims 2, 9-11 and 17 are objected to because apparently they should be

dependent upon claim 9.

      As per claim 2, 9,10,11,17, this claim recites limitation "integer N times" on line

2. It is not defined.

As per claim 17, this claim recites limitation "K times" on line 2. It is not defined.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1-4,6-14,16-19, 21-23 and 25-26 are rejected under 35 U.S.C 103(a) as

being unpatentable over Heard et al (US 2006/0236363) (hereinafter Heard) in view of

Dal Canto et al (US 2003/0217166) (hereinafter Dal) further in view of Patel (SU

6591364)(hereinafter Patel).

As per claim 1, Heard discloses " a data transmitting apparatus comprising:

"a command transmission transmitting unit configured to transmit a response

request command to a data receiving apparatus" as (par 0074, the device initiates the

challenge [a response request command] and sent to the gatekeeper   ) ;

"a control unit configured to receive a response message to the response request

command from the data receiving apparatus" as (par 0074, the gatekeeper sends a

response to the device),

" the response message including authentication data based on shared data shared with said data receiving apparatus" as (par 0074, the calculated value of response of shared key and challenge value);

"an expected value generation unit configured to generate an expected authentication value based on the shared data (par 0074, the gatekeeper compute the expected answer with shared key and challenge)

"an authentication unit configured to produce an authentication result for said data receiving apparatus based on the expected value generated by said expected value generation unit and said authentication data in the response message" as (par 0074-0075, the gatekeeper authenticates the device based on expected answer and the gatekeeper compute the expected answer with shared key and challenge, computed response includes shared key and challenge).

Heard fails to disclose " an expected value generation unit configured to generate an expected authentication value based on sequence number, the sequence number indicating an ordinal position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit;

a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message; and

a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time".

However, Dal discloses "a measurement unit configured to measure a response time between transmitting the response request command and receiving the response message (par 0059, user request for digital service, the round-trip delay or response time of user request and the received a response from the service center); and

a judgment whether unit configured to judge if a subsequent data transmission to said data receiving apparatus is granted based on the authentication result and the response time" (par 0059, authentication service authenticates a client device for having service form the service center. authentication service provides an authentication result of client device bases on client profile information which contains information relating to the client device type , attached peripheral devices, location, etc).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the claimed invention by modifying the method of Heard, based on the teachings of Dal, because doing so, would improve authorization for services.

The combination of Heard and Dal fail to disclose "an expected value generation unit configured to generate an expected authentication value based on sequence number, the sequence number indicating an ordinal position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit".

However, Patel discloses "an expected value generation unit configured to generate an expected authentication value based on sequence number, the sequence number indicating an ordinal position of the response request command in a sequence of response request commands to be transmitted by the command transmission unit" as (column 3, lines 47-59, column 4, lines 1-20, Mobile generates KCF ssda (Type, 0, Cm, Rn) [expected value] for authentication. Cm is the count value [sequence number] , which is related to Rn that is send to the mobile as a challenge. Cm is incremented during the challenge response. This incremented value of Cm [counter] is an ordinal number [ordinal position] of the mobile device]. Type data is shared data between Mobile device and VLR. VLR calculates KCF ssda (Type, 0, Cm, Rn) [expected value] for mutually authentication).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to implement the claimed invention by modifying the method of Heard in view of Dal, based on the teachings of Patel, because doing so, would prevent unauthorized access for services.

As per claim 2, Heard in view of Dal in view of Patel disclose "said command transmission unit is further configured to transmit said response request command a maximum of N times" as (Patel, column 3, lines 47-59, column 4, lines 1-20, VLR sends Rn as a challenge [a response request command] to the mobile device. Rn

where is n represents times); "said control unit is further configured to receive the response messages from the data receiving apparatus for each of the N transmitted response request commands" as (Patel, column 3, lines 47-59, column 4, lines 1-20, VLR receives a response from the mobile); and "said authentication unit is further configured to produce authentication results based on said authentication data in each received response message" as (Patel, column 3, lines 47-59, column 4, lines 1-20, VLR authenticates Mobile device bases on Rn and Cm and Type [authentication data], this data has been exchanged via response message from mobile device) .

As per claim 3, this claim is directed to a data transmission method and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 4, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 6, this claim is directed to a data receiving apparatus and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 7, Heard in view of Dal in view of Patel disclose "said shared data is a quasi random number transmitted from said data transmitting apparatus before said

response request command is transmitted" (Heard, par 0074, shared key [shared data]

is transmitted before a challenge [response request command]) ; and

"said authentication data generation Unit is further configured to subject said

quasi random number to a Keyed-Hash process to produce a Hash value that is used

as said authentication data" (Heard, par 0074, key can be input to a hash algorithm as

MD5 as a authentication data).

As per claim 8, Heard in view of Dal in view of Patel disclose "said

authentication data generation unit is further configured to execute a Keyed-Hash

process relative to said quasi random number and information specific to the

information processing apparatus to produce a Hash value that is used as said

authentication data" as (Patel, column 3, lines 47-59, column 4, lines 1-20, Keyed

cryptographic function KCF to Rn and Type data that represents mobile registration, etc

[information specific to the processing apparatus]. Hash of KCF is the authentication

data).

As per claim 9, Heard in view of Dal in view of Patel disclose "said command

receiving unit is further configured to receive said response request command from

said data transmitting apparatus a maximum of N times" as (Patel, column 3, lines 47-

59, column 4, lines 1-20, mobile receives Rn as challenge [response request

command] from the VLR of n times); said" authentication data generation unit is

further configured to execute said predetermined process relative to said shared data

before a first one of said response request command commands is received from said

data transmitting apparatus and further configured to generate N sets of said

authentication data corresponding to said N received response request Commands" as

(Patel, column 3, lines 47-59, column 4, lines 1-20, VLR does KCF [predetermined

process] on Type, Rn , Cm [shared data] and Mobile device does KCF [predetermined

process] on Type, Rn , Cm [shared data]. Both devices compute n times of

authentication data related to the Rn as a challenge   ); and "said transmission unit is

further configured to transmit said response message generated by said response

message generation unit to said data transmitting apparatus, said response message

including the N sets of said authentication data in a sequence agreed beforehand with

said data transmitting apparatus" as (Patel, column 3, lines 47-59, column 4, lines 1-

20, mobile device sent response bases on challenge Rn of n times, response from

mobile device sent authentication data to the VLR, authentication data includes Cm [a

sequence] for both devices).

As per claim 10, Heard in view of Dal in view of Patel disclose "said

authentication data generation unit is further configured to divide the data obtained by

subjecting said shared data to said process into a plurality of data pieces and further

configured to generate the N sets of said authentication data from the divided data" as

(Patel, column 3, lines 47-59, column 4, lines 1-20, Mobile and VLR produces KCFssda

(Type, 0, Cm, Rn) as authentication data of sets of Rn challenge from shared data

Type[divided data between mobile and VLR]).

As per claim 11, Heard in view of Dal in view of Patel disclose "said authentication data generation means unit is further configured to generate the N sets of said authentication data based on data obtained at each process of repetitively executing said predetermined process relative to said shared data" as (Patel, column 3, lines 47-59, column 4, lines 1-20, Mobile and VLR produces KCFssda (Type, 0, Cm, Rn) as authentication data of sets of Rn challenge from shared data Type[divided data between mobile and VLR] , Mobile and VLR would produces KCFssda (Type, 0, Cm, Rn) as an authentication data for each challenge [shared data] at any execution).

As per claim 12, Heard in view of Dal in view of Patel disclose "said transmission unit is further configured to transmit the response message to said transmitting apparatus when said response request command is received from the data transmitting apparatus, said response message containing new authentication data generated from said authentication data and information contained in said response request command" as (Patel, column 3, lines 47-59, column 4, lines 1-20, VLR sends Rn to Mobile and Mobile sends response to VLR with New authentication value [KCFssda(Type, 0, Cm, Rn)] for each Type, Cm and Rn, Rn [information] is as a response request command).

As per claim 13, this claim is directed to a data reception method and contains limitations that are substantially similar to those recited in claim 6 above, and accordingly is rejected for similar reasons.

As per claim 14, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim **6** above, and accordingly is rejected for similar reasons.

As per claim 16, this claim is directed to an information transmitting apparatus and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 17, this claim is directed to an information transmitting apparatus and contains limitations that are substantially similar to those recited in claim **2** above, and accordingly is rejected for similar reasons.

As per claim 18, this claim is directed to a data transmission method and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 19, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 21, this claim is directed to a data receiving apparatus and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 22, this claim is directed to a data reception method and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 23, this claim is directed to a computer program and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 25, this claim is directed to a communication system and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

As per claim 26, this claim is directed to a communication system and contains limitations that are substantially similar to those recited in claim **1** above, and accordingly is rejected for similar reasons.

Examiner Notes

7.   Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

8.   The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

9.   The following reference teaches execution of trial data.

US 7058414

10.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314 and Fax number is (571)-270-8314. The examiner can normally be reached on Monday through Friday 9:30 AM - 5:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865.   The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.   Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ABU SHOLEMAN/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437